UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/923,213	08/06/2001	Lynn Henry Wheeler	10399-34384	8986

24728 7590 10/10/2007

MORRIS MANNING MARTIN LLP
3343 PEACHTREE ROAD, NE
1600 ATLANTA FINANCIAL CENTER
ATLANTA, GA 30326

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2137	
MAIL DATE	**DELIVERY MODE**
10/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/923,213	WHEELER ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 21-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 21-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/27/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-5 and 21-32 are pending.

2. Amendment filed 08/27/2007 has been received and considered.

Claim Rejections - 35 USC § 112

3. The rejections under 35 U.S.C. 112 have been withdrawn based on the filed amendment.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 21, 25 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (US 5422953) in view of Rosen (US 5557518).

As per claims 1 and 32, Fischer discloses a method of manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified, comprising

the steps of: a. creating a public-private key pair within the secure environment, the private key for utilization in generating a digital signature for an electronic message, the public key exportable for use by third parties in connection with authenticating the electronic message (see column 4 lines 23-34 and Fig 2); b. storing the private key within the device against the divulgement thereof by the device (see column 3 lines 31-38); and c. linking the public key with other information by storing the public key and the other information in a database (see column 2 lines 19-37 and column 6 lines 10-65) using the device to generate digital signatures verifiable by the third party using the public key and other information (see column 11 line 56 through column 12 line 25).

Fischer fails to explicitly disclose that the device is manufactured in a secure environment and that the database is securely linked within the secure environment.

However, Rosen teaches manufacturing a device in a secure environment (see column 11 lines 6-13), releasing the device (see column 11 lines 26-30) and a database containing linked information within a secure environment (see column 10 lines 56-67 and Figure 5 and column 11 lines 14-30).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to manufacture the device

of Fischer in a secure environment and for the secure database to be within the secure environment.

Motivation to do so would have been to guarantee the protocols and physical protection of each device (see column 11 lines 6-13) and to provide trusted certificates to the trusted devices (see column 10 lines 56-67).

As per claims 2-3, the modified Fischer and Rosen system discloses each public-private key pair is created within each device based on a random number produced by a random number generator disposed within each device and each digital signature generated by each device is a random number (see Rosen column 9 lines 54-66).

As per claim 4, the modified Fischer and Rosen system discloses the other information comprises respective security features and a manufacturing history of each device (see Fischer column 6 lines 10-65 and Rosen Figure 34 and respective description).

As per claim 5, the modified Fischer and Rosen system discloses identifying a particular manufactured device by authentication a message using one of said linked public keys, a digital signature for the message having been generated by the particular manufactured device (see Fischer column 7 lines 20-34).

As per claim 21, the modified Fischer and Rosen system discloses the public key and information linked therewith is obtained from a secure entity (see Fischer column 4 lines 29-34 and Rosen column 10 lines 56-67).

As per claim 25, the modified Fischer and Rosen system discloses the public key and the other information stored in the database for each user further includes user-specific information (see Fischer column 2 lines 19-37).

6. Claims 22-24 and 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Fischer and Rosen system in view of Ramasubramani (US 6233577).

As per claim 22, the modified Fischer and Rosen system fails to disclose the other information stored in the database includes the identity of a plurality of third-parties with which an account is maintained, the accounts being identified by one of a plurality of third-party account identifiers.

However, Ramasubramani teaches a system in which certificates are stored and maintained for a plurality of third-parties in a centralized database, the accounts being identified by one of a plurality of third-party account identifiers (see Figure 4B).

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of

Ramasubramani with those of the modified Fischer and Rosen system because doing so makes the system more robust and efficient by allowing for centralized storage and retrieval of certificates for a plurality of users.

As per claims 23-24 and 27-28, the modified Fischer, Rosen, and Ramasubramani system discloses the public key linked account information of the users is indexed in the database by unique account identifiers such that the public key linked account information for a user is retrieval from the database based on the account identifier (see Ramasubramani Fig 4B).

7. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Fischer and Rosen system in view of Schneier (Schneier, Bruce. Applied Cryptography. John Wiley & Sons. 1996. pages 185-187).

As per claim 26, the modified Fischer and Rosen system fails to disclose the user-specific information includes the name and address of the user.

However, Schneier discloses the well-known idea that a certificate may disclose the name and address of a user (see page 186).

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneier with the modified Fischer and Rosen system and include

the name and address of a user for further identification purposes.

8. Claims 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Fischer and Rosen system in view of Menezes (Menezes, Alfred J. Handbook of Applied Cryptography. CRC Press. 1997. pages 25-32; 546-548; 572-577).

As per claim 29, the modified Fischer and Rosen system discloses a) receiving an EC, the EC including an account identifier and a message including the new public key and a digital signature therefor (see Fischer column 2 lines 19-37); but fails to disclose authenticating the message of the EC using the public key associated with the account in the database identified by the account identifier, and upon successful authentication thereof; c) sending an EC to each of the third-parties, each EC including the new public-key and the third-party account identifier for the respective third-party maintained in the database and associated with the account identified by the account identifier.

However, Menezes discloses authenticating the message of the EC using the public key associated with the account in the database identified by the account identifier, and upon successful authentication thereof (see pages 25-26); c) sending

an EC to each of the third-parties, each EC including the new public-key and the third-party account identifier for the respective third-party maintained in the database and associated with the account identified by the account identifier (see page 576).

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of the modified Fischer and Rosen system because doing so provides a number of benefits to the system, including making the system more robust and secure by providing for authentication of a user message.

As per claim 30, the modified Fischer, Rosen and Menezes system discloses the step of digitally signing a message involving the new public key of the user and a third-party account identifier (see Fischer column 2 lines 19-37).

As per claim 31, the modified Fischer, Rosen and Menezes system discloses the step of sending the EC received from the user to each of the third-parties (see Menezes page 576).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple

assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-5 and 21-31 of the instant application are rejected by U.S. Patent No. 6,915,430, U.S. Patent No. 6,892,302, and copending U.S. Patent Application No. 10/248,626. A discussion of how independent claim 1 is met by each of the four cases is cited below. The examiner notes that the dependent claims are met by the four cases as well but haven't been specifically discussed for the sake of brevity.

Claims 17 of U.S. Patent No. 6,915,430 contains every element of claim 1 of the instant application and as such anticipates claim 1 of the instant application. Claim 18 of U.S. Patent No. 6,892,302 contains every element of claim 1 of the instant application and as such anticipates claim 1 of the instant application. Claim 28 of copending U.S. Patent No. 7,047,414 contains every element of claim 1 of the instant

application and as such anticipates claim 1 of the instant application.

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus)." Eli Lilly and Company v Barr Laboratories, Inc., United States Court of Appeals for the Federal Circuit, On Petition for Rehearing en Banc (Decided: May 30, 2001).

NOTE: The double patenting rejection under application 10/248,629 (now US 6959381) has been withdrawn based on applicant's remarks.

Examiner also thanks applicant for indicating a willingness to file a terminal disclaimer upon allowance of claims in the present application.

Response to Arguments

9. Applicant's arguments filed 08/27/2007 have been fully considered but they are not persuasive. Applicant's argue that Rosen relates to providing certificates to trusted devices and not for providing devices for use in message authentication; Fischer fails to disclose linking a public key with other information in a database; Rosen teaches the primary trusted server stores the keys of the trusted servers, not the devices; the public keys are not stored with "other information"; and the claims are directed to an AADS authentication model while the art presented relates to CADS models.

With respect to Applicant's argument that Rosen relates to providing certificates to trusted devices and not for providing devices for use in message authentication, the cited portions of Rosen relate to the secure manufacturing of devices and Fischer is relied upon to teach the specific device for message authentication.

With respect to Applicant's argument that Fischer fails to disclose linking a public key with other information in a database, the key pair is created and stored and therefore linked to the device that stores them, furthermore, the public key is linked to the private key which is stored in the device and therefore must identify the "other information".

Additionally, Rosen teaches the public key is sent with an ID and combined into a certificate stored on a server. Therefore Rosen also teaches the public key is linked with other information in a database.

With respect to Applicant's argument that Rosen teaches the primary trusted server stores the keys of the trusted servers, not the devices, the Examiner agrees with this statement. However, the trusted servers store the public keys of the devices (see column 11 lines 14-25). This storing is additionally performed during the manufacturing in the secure environment.

With respect to Applicant's argument that the public keys are not stored with "other information" as described above, each of the public keys of Rosen are stored with an ID in a certificate. Therefore, the public keys are stored with other information.

With respect to Applicant's argument that the claims are directed to an AADS authentication model while the art presented relates to CADS models, there is nothing in the claims preventing a certificate authority digital signature model from rendering the claims unpatentable. Applicant contends that because the third party authenticates electronic messages based on a public key of the device and the other information.

However, Fischer uses this same method of authenticating messages (see Figure 5 and corresponding description) as the public key is contained in the certificate and the certificate has other information to verify authenticity of the message and public key itself. The mere fact that there is no certificate exchange or authority required in the specification is not relevant as these are not claimed limitations and the claims are given their broadest reasonable interpretation.

The arguments incorporated from the previously filed Appeal Brief are moot based on the previously present new grounds of rejection or the above response.

Examiner notes and appreciates Applicant's willingness to file a terminal disclaimer. If Applicant files a proper terminal disclaimer the double patenting rejections would be withdrawn.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action

is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER